

УДК 343.4 : 343.431 : 004.056.53

Сергій Віталійович КАВУН,

Prof., Dr.Sc.(Econ), Ph.D.(CS&E), начальник відділу інформаційних технологій Харківського навчально-наукового інституту Державного вищого навчального закладу «Університет банківської справи»

Наталія Олексіївна ВАКУЛЕНКО,

студентка Харківського навчально-наукового інституту Державного вищого навчального закладу «Університет банківської справи»

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Безперечно, на сучасному етапі розвитку людського суспільства важливим стратегічним ресурсом, що потребує охорони, є інформація, яка містить надзвичайно широкий спектр зведень: від простих даних про громадян країни до стратегічних державних програм. Тому ці дані все частіше стають предметом злочинних зазіхань. Комплексне і широкомасштабне використання інформаційних технологій на основі персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем забезпечило людству вихід на новий етап свого розвитку – етап інформаційного суспільства. Як наслідок – поява нового виду злочинності – комп'ютерної, або кіберзлочинності [7].

Зростання обсягів інформації, комп'ютерних мереж та кількості користувачів, спрощення їх доступу інформації, що циркулює мережами суттєво підвищує ймовірність розкрадання або руйнування цієї інформації.

В даний час значущість проблеми захисту інформаційних ресурсів, у тому числі особистих, визначається наступними факторами:

- розвитком світових і національних комп'ютерних мереж і нових технологій, які забезпечують доступ до інформаційних ресурсів;
- перекладом інформаційних ресурсів на електронні носії й концентрацією їх в інформаційних системах;
- підвищенням «ціни» створюваної та накопиченої інформації, яка є реальним ресурсом соціально-культурного та особистісного розвитку;

- розробкою і вдосконаленням інформаційних технологій, які можуть ефективно використовуватися кримінальними структурами.

Комп'ютерна злочинність стала справжнім бичем економіки розвинених держав. Так, наприклад, 90% фірм і організацій у Великобританії в різний час ставали об'єктами електронного піратства або перебували під його загрозою, у Нідерландах жертвами комп'ютерної злочинності стали 20% різного роду підприємств. У ФРН з використанням комп'ютерів щорічно викрадається інформація на суму 4 млрд євро, а у Франції - 1 млрд євро.

Про проблему торгівлі людьми, два основних моменти: її суспільна небезпечність і її поширеність у світі.

Основними проявами суспільної небезпеки торгівлі людьми, у свою чергу, ґрунтуючись на тому, що загальновідомо про торгівлю, і на те, що доведено в науці, слід визнати:

- перетворення людини в річ, нехтування його прав і свобод;

- первинну і вторинну криміногенність торгівлі людьми:

- первинна: сама торгівля людьми - злочинне діяння;

- вторинна: торгівля людьми - криміногенний фактор, який манить вчинення інших злочинів;

- порушення норм міжнародного та національного законодавства.

Про поширеність такого явища, як торгівля людьми, у світі можна судити на підставі експертних даних, і (або) на підставі статистичних даних про вчинені злочини. Експертні дані зводяться до наступних:

- кількість жертв торгівлі людьми обчислюється в межах від 700 тисяч до 2-4 мільйонів (за даними Уряду США);

- щорічно у світі продають 1,2 мільйона дітей (за даними ЮНІСЕФ);

- тільки в країнах колишнього СРСР щороку жертвами торгівлі людьми стають від 20 тисяч до 700 тисяч чоловік;

- щорічний дохід від торгівлі людьми у світі становить від 6-8 млрд доларів (за даними Інтерполу) до 19 млрд доларів (дані експертів).

Можна виділити основні органи, які займаються розробленням і впровадженням профільних норм міжнародного права у напрямі протидії торгівлі людьми. До них ми включаємо:

- Організацію Об'єднаних Націй;

- Європейський Союз;

- Раду Європи;
- Організацію з безпеки й співробітництва в Європі (ОБСЕ);
- міжнародні міжурядові та неурядові організації, такі як, наприклад, Міжнародна Ліга жінок за мир і свободу, Міжнародна Демократична Федерація жінок, Всесвітня організація за виживання (The Global Survival Network), Фонд проти торгівлі людьми (The Foundation Against Trafficking) та багато інших.

Вважаємо, що розробка та прийняття міжнародних конвенцій, декларацій, інших міжнародно-правових документів у сфері прав людини сприяє загальному визнанню вимог про рівноправність статей. Міжнародні акти, зобов'язуючи держави здійснювати проголошені в них права, виступають як додаткові міжнародно-правові гарантії захисту прав людини. При цьому підкреслимо, що, по-перше, безпосередня регламентація правового становища людини є компетенцією держави та залежить від її соціально-економічного розвитку; по-друге, дотримання міжнародних норм про захист прав, їх впровадження в життя значною мірою залежить від активності самих людей.

На сьогодні приблизно 180 країн мають законодавство, що дозволяє протидіяти проявам торгівлі людьми. Складність та багатогранність цього явища обумовили різні підходи до криміналізації діяння кримінальні кодекси різних країн трактують цей злочин по-різному, в одних країнах торгівля людьми виділена в окремий склад злочину, в інших не виділена в окремий склад та переслідується в рамках інших наявних законів або не переслідується зовсім.

Список використаних джерел:

1. Назаренко Г. В. Кримінальне законодавство: навч. посібник. М. : Нове видання, 2008. 214 с.
2. Моделі кіберпреступностей. URL: <https://goo.gl/VxC5Xu> (дата звернення: 23.10.2017).
3. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. URL: <https://goo.gl/c8heHE> (дата звернення: 23.10.2017).
4. Міжнародні стандарти протидії торгівлі людьми / GOAL. 2014. URL: <https://goo.gl/F6D9sp> (дата звернення: 23.10.2017).
5. Tosin Osasona. Time to Reform Nigeria's Criminal Justice System, Journal of Law and Criminal Justice. December 2015, Vol. 3, No. 2, pp. 73-79.

6. Ramsaroop P. Cybercrime, Cyberwarfare, Terrorism, and Sabotage: Critical Issues in Data Protection for Health Services Information Pan American Health Organization. Washington, D.C.: PAHO, 2003. 85 p.
7. Струков В. М. До визначення напрямів протидії кіберзлочинності URL: <http://bit.ly/2imbPQe> (дата звернення: 23.10.2017).

Одержано 01.11.2017

УДК 343.98

Сергій Павлович ЛАПТА,

кандидат юридичних наук, доцент, доцент кафедри криміналістики та судової експертології факультету №1 Харківського національного університету внутрішніх справ

ФБР У БОРОТБІ З КІБЕРЗЛОЧИННІСТЮ

Проблема боротьби зі злочинами у кіберпросторі наразі визнається одною із найгостріших серед проблем боротьби зі злочинністю. Викликано це рядом факторів, які у значній мірі ускладнюють протидію кіберзлочинності. Для того щоб розпочати «бізнес» злочинцям іноді потрібні лише незначні грошові кошти. Злочинці можуть «атакувати» одночасно значну кількість потенційних жертв, рахунок яких іноді йде на сотні тисяч. Відповідно, якщо злочинна діяльність направлена на отримання кримінальних прибутків, вони значно збільшуються порівняно з іншими, традиційними способами. Так, у ході масованої кібератаки із застосуванням вірусу-вимагача Petya, яка відбулася 27 червня 2017 року, тільки в Україні постраждало близько 12,5 тисяч комп'ютерів та вийшла з ладу система радіаційного моніторингу Чорнобильської АЕС. У світі жертвами стали такі гіганти, як британська рекламна компанія WPP; датський бізнес-конгломерат Maersk, який є найбільшим оператором корабельної контейнерної доставки у світі; німецька логістична компанія DHL; американська продуктова компанія Mendeleez; група американських госпіталів Heritage Valley Health System. та багато інших [1]. Перед цим, 12 травня 2017 року від вірусу-вимагача WannaCry постраждало більше 300 тисяч комп'ютерів у 150 країнах світу, а злочинці отримали понад 100 тисяч доларів [2].

Є й інші фактори, що ускладнюють протидію кіберзлочинності порівняно із злочинністю традиційною:

- повністю виключений реальний контакт злочинців і жертв;